Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Original) A method processing one or more files using a security application, the method comprising:

connecting the client to a proxy server, the proxy server being coupled to one or more NAS servers;

requesting for a file from a client to the proxy server;

authenticating a requesting user of the client;

authorizing the requesting user for the file requested;

requesting for the file from the one or more NAS servers after authenticating and authorizing;

requesting for the file from the one or more storage elements;

transferring the file from the one or more storage elements through the NAS server to the proxy server;

determining header information on the file at the proxy server;

identifying a policy based upon the header information at the proxy server;

processing the file according to the policy, the processing including decompressing the file, decrypting the file, and verifying the file; and

transferring the processed file to the user of the client.

2. (Original) The method of claim 1 wherein the file comprises retrieval and verification information.

3. (Original) The method of claim 1 wherein the decryption is provided by a NIST approved process.

4. (Original) The method of claim 1 wherein the NIST approved process is selected from AES and Triple-DES.

5. (Original) The method of claim 1 wherein the verifying comprises processing a keyed message authentication code.

6. (Original) The method of claim 5 wherein the keyed message authentication code is generated using a SHA-1 or MD-5 or SHA-512.

7. (Original) The method of claim 1 further comprising determining one or more statistics in a database on a security device.

8. (Original) The method of claim 7 wherein the database is a secure catalog database.

9. (Original) The method of claim 8 further comprising using the secure catalog database to detect an intrusion.

10. (Original) The method of claim 1 further comprising adding information associated to positional integrity to the file.

11. (Original) The method of claim 1 further comprising generating a signature record on the file to detect any modification of the file.

12. (Original) The method of claim 1 further comprising identifying a number of blocks stored within a database, the database including the file.

13. (Withdrawn) A system for providing security on a network attached storage, the system comprising:

a directed proxy server coupled to a databus, the databus being coupled to a plurality of clients, the directed proxy server being adapted to add header information and to add trailer information on a file by file basis, the directed proxy server being adapted to provide policy information on either or both the header information and the trailer information;

a NAS server coupled to the directed proxy server; and

one or more storage device coupled to the filer.

14. (Withdrawn) The system of claim 13 wherein the directed proxy server communicates to the filer using an access protocol selected from NFS or CIFS format.

15. (Withdrawn) The system of claim 13 wherein the directed proxy sever is transparent to a user.

16. (Withdrawn) The system of claim 13 wherein the NAS server is transparent to the plurality of clients.

17. (Withdrawn) The system of claim 13 wherein the directed proxy server operates at a wire speed to add header information and trailer information.

18. (Withdrawn) The system of claim 13 wherein the directed proxy server is adapted to maintain a plurality of security keys, one or more of the keys is associated with a group of the files.

19. (Withdrawn) The system of claim 13 wherein the directed proxy server is adapted to maintain a plurality of security keys, one or more of the keys is associated with a user.

20. (Withdrawn) The system of claim 13 wherein the policy information is associated with a service, the service is selected from an encryption process, a decryption process, an authentication process, an integrity process, a compliance process, an intrusion detection process, or a promotion process.

21. (Withdrawn) A method processing one or more files using a security application, the method comprising:

connecting a security device to a NAS server, the NAS server being coupled to one or more storage elements;

detecting one or more changed files on the NAS server;

detecting one or more portions of the one or more files that have been changed;

determining a policy information for at least one of the changed files to determine a security attribute information;

generating header information for the changed file;

attaching the header information on the changed file;

processing at least one portion of the changed file according to the policy information, the processing including:

compressing the portion;

encrypting the portion;

generating one or more message authentication codes associated with the portion of the changed file;

transferring the changed file to one or more of the storage elements.

22. (Withdrawn) The method of claim 21 wherein the processing is provided at wire speed.

23. (Withdrawn) The method of claim 21 wherein the one or more of the storage elements is a storage area network.

24. (Withdrawn) The method of claim 21 wherein the transferring of the changed file is provided via SCSI interface.

25. (Withdrawn) The method of claim 21 wherein the policy information is provided in a library.

26. (Withdrawn) The method of claim 21 wherein the encrypting is decrypting.

27. (Withdrawn) A method processing one or more files using a security application, the method comprising:

connecting the client to proxy server, the proxy server being coupled to one or more NAS servers;

transferring a file from a client to the proxy server;

authenticating a user of the client;

authorizing the user for the file requested;

processing the file using a keyed message authentication integrity process;

generating header information for the file;

attaching the header information on the file;

transferring the file to one or more of the NAS servers;

transferring the file from the one or more NAS servers to one or more storage elements.

28. (Withdrawn) The method of claim 27 further comprising encrypting the file using a key size of at least 128 bits to form an encrypted file.

29. (Withdrawn) The method of claim 28 wherein the encrypting is provided using a NIST approved process.

30. (Withdrawn) The method of claim 28 wherein the encrypting is provided using AES-128, AES-192, AES-256, Triple-DES.

31. (Withdrawn) The method of claim 27 wherein the keyed message authentication integrity process is provided by SHA-1, SHA-2, MD-5.

32. (Withdrawn) The method of claim 27 wherein the processing is provided at wirespeed, the wirespeed being greater than 1 Gigabit/second.

33. (Withdrawn) The method of claim 27 wherein the authenticating, authorizing, processing, generating, and attaching are provided at the proxy server.

34. (Withdrawn) The method of claim 27 wherein the header information comprises at least one element selected from a time stamp, Encrypted Data Encrypted Key, Encrypted Data Hash MAC key, and File attributes.

35. (Withdrawn) The method of claim 27 further comprising transferring the file to one or more to other storage elements.

36. (Withdrawn) A method processing one or more files using a security application, the method comprising:

connecting the client to server, the server being coupled to one or more storage elements;

transferring a file from a client to the server;

authenticating a user of the client;

authorizing the user for the file requested;

processing the file using a keyed message authentication integrity process;

generating header information for the file;

attaching the header information on the file; and

transferring the file to one or more of the storage elements.

37. (Withdrawn) The method of claim 36 further wherein the one or more storage elements comprises one or more NAS servers to one or more storage elements.

38. (Withdrawn) The method of claim 36 further comprising encrypting the file using a key size of at least 128 bits to form an encrypted file.

39. (Withdrawn) The method of claim 38 wherein the encrypting is provided using a NIST approved process.

40. (Withdrawn) The method of claim 38 wherein the encrypting is provided using AES-128, AES-192, AES-256 or Triple-DES.

41. (Withdrawn) The method of claim36 wherein the keyed message authentication integrity process is provided by SHA-1, SHA-2, MD-5.

42. (Withdrawn) The method of claim 36 wherein the processing is provided at wirespeed, the wirespeed being greater than 1 Gigabit/second.

43. (Withdrawn) The method of claim 36 wherein the authenticating, authorizing, processing, generating, and attaching are provided at the proxy server.

44. (Withdrawn) The method of claim 36 wherein the header information comprises at least one element selected from a time stamp, Encrypted Data Encrypted Key, Encrypted Data Hash MAC key, and File attributes.

45. (Withdrawn) A method for providing secured storage of data, the method comprising:

providing a key encryption key;

storing the key encryption key on a system;

storing a message authentication code generating key on the system;

decrypting a file encryption key with the key encryption key;

decryption a file message authentication code generating key with the key encryption key;

using the file encryption key to decrypt data stored on a server or encrypt data originated by a user on a client;

generating a message authentication code for a header of the file with the message authentication code generating key; and

using the file message authentication code generating key to generate one or more message authentication codes block by block in the file.

46. (Withdrawn) The method of claim 45 wherein the file encryption key is provided in the file.

47. (Withdrawn) The method of claim 45 wherein the file message authentication key is provided in the file.

48. (Withdrawn) The method of claim 45 wherein the file message authentication key verifies content of data of the file upon a read process.